Sistem upravljanja varovanja informacij - SUVI

Standardizacija

- Sistemov upravljanja varovanja informacij - SUVI
  Information Security Management Systems - ISMS
- družina standardov
  - ISO/IEC 27001
  - Zamenjuje ISO/IEC 17799:2000
  - sestavljen iz dveh delov
    - 1. del - zahteve
    - 2. del - praksa

Namen standarda

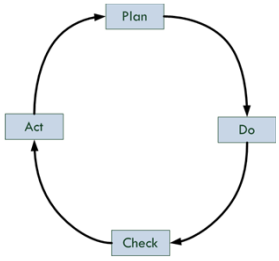
- podaja model za
  - določitev
  - vzpostavitev
  - delovanje
  - spremljanje
  - pregled
  - vzdrževanje
  - izboljševanje
- sistema upravljanja varovanja informacij (SUVI)

Procesni pristop

- uporablja procesni pristop
- organizacija mora identificirati in upravljati mnoge aktivnosti
- vzpostavitev sistema procesov v organizaciji skupaj z identifikacijo in interakcijo teh procesov in njihovim upravljanjem je “procesni pristop”

PDCA model

- Plan-Do-Check-Act
- s poudarkom na:
  - razumevanjem varnostnih zahtev organizacije
  - implementacijo in delovanjem kontrol za upravljanje tveganj
  - spremljanje in pregled učinkovitosti in uspešnosti SUVI in
  - neprestanem izboljševanju, ki temelji na objektivnih meritvah.



Vzpostavitev in upravljanje SUVI

- definiranje obsega in mej SUVI glede na:
  - značilnosti poslovanja
  - organizacijo
  - lokacijo
  - sredstva in tehnologijo

Vzpostavitev in upravljanje SUVI

- definiranje SUVI politike, ki:
  - vključuje ogrodje za vzpostavitev ciljev
  - upošteva poslovne cilje, predpise in pogodbene obveznosti
  - je usklajena s poslovnimi cilji
  - vsebuje kriterije za ocenjevanje tveganj
  - jo potrdi vodstvo.

Vzpostavitev in upravljanje SUVI

- definiranje pristopa k obravnavanju tveganj
  - identifikacija metodologije ocene tveganj
  - izdelava kriterijev za sprejemanje tveganj
- metodologija mora zagotavljati rezultate, ki jih je možno reproducirati in so primerljivi

Vzpostavitev in upravljanje SUVI

- identifikacija tveganj:
  - identifikacija sredstev
  - identifikacija pretenj tem virom
  - identifikacija ranljivosti, ki bi jih lahko izrabile pretnje
  - identifikacija učinkov, ki jih ima izguba zaupnosti, integritete in dostopnosti sredstev

Vzpostavitev in upravljanje SUVI

- analiza in ocena tveganj
  - analiza vplivov na poslovanje zaradi incidentov
  - realna ocena verjetnosti incidenta
  - določanje stopnje tveganja
  - odločanje ali je tveganje sprejemljivo

Vzpostavitev in upravljanje SUVI

- identifikacija in ocenitev možnosti za naslavljanje tveganj
  - vzpostavitev kontrol
  - sprejemanje tveganj
  - izogibanje tveganj
  - prenos tveganj

Vzpostavitev in upravljanje SUVI

- določitev kontrolnih ciljev in kontrol
- odobritev vodstva za preostala tveganja
- pridobitev podpore vodstva za vpeljavo in izvajanje SUVI

Vpeljava in izvajanje SUVI

- izdelava in vpeljava načrta zmanjševanja tveganj
- vpeljava kontrol
- definicija metrik
- vpeljava programov ozaveščanja in izobraževanja
- upravljanje izvajanja SUVI
- upravljanje sredstev SUVI
- vzpostavitev postopkov in kontrol upravljanja incidentov

Spremljanje in pregled SUVI

- izvajanje postopkov spremljanja in pregledov
- redni pregledi učinkovitosti SUVI
- merjenje učinkovitosti kontrol
- periodični pregled ocene tveganj
- interna periodična revizija SUVI
- periodični vodstveni pregled SUVI
- posodabljanje varnostnih načrtov
- beleženje pomembnih dogodkov

Vzdrževanje in izboljšave SUVI

- vpeljava identificiranih izboljšav SUVI
- sporočanje o uspešnosti vpeljave pristojnim
- zagotavljanje, da izboljšave dosežejo načrtovane cilje

Informacija

- je sredstvo, ki je tako kot ostala poslovna sredstva ključen za delovanje organizacije
- morajo biti primerno zaščitene
- še pomembneje je to v vedno bolj povezanih poslovnih okoljih

Oblika informacij

- informacija lahko obstaja v več oblikah:
  - tiskana
  - zapisana na papir
  - shranjena elektronsko
  - poslana po pošti
  - poslana z elektronskimi sredstvi
  - prikazana v filmih
  - povedana v pogovoru
- ne glede na obliko jo moramo zaščititi

Informacijska varnost

- je zaščita informacij pred vrsto pretenj, z namenom zagotoviti
  - neprekinjenost poslovanja
  - zmanjšanje poslovnih tveganj
  - Optimiranje povračilo investicij

Kako doseči informacijsko varnost?

- z vzpostavitvijo primernega nabora kontrol
  - politike
  - procese
  - postopke
  - organizacijske strukture
  - funkcije programske opreme
  - funkcije strojne opreme

Kontrole

- kontrole morajo biti:
  - vzpostavljene
  - vpeljane
  - nadzorovane
  - preizkušene
  - izboljšane

Zakaj potrebujemo informacijsko varnost?

- organizacije in njihovi informacijski sistemi, omrežja se soočajo z varnostnimi pretnjami:
  - računalniško podprte prevare
  - vohunjenje
  - sabotaže
  - vandalizem
  - požari
  - poplave

Povečuje se število incidentov

- vzroki škode:
  - zlonamerna koda
  - računalniški vdori (hekerji)
  - napadi preprečevanja dostopa do storitev
- vse pogostejši napadi
- vse več napadov ima točno določen cilj (motiv)
- napadi so vse bolj izpopolnjeni

Področja informacijske varnosti

- pomembna je za javni in zasebni sektor
- za kritično infrastrukturo
- mnogi informacijski sistemi niso bili načrtovani z upoštevanjem varnosti
  - tehnična zaščita mora biti podprta z vodenjem in postopki

Vpleteni v informacijsko varnost

- vsaj vsi zaposleni!
- lahko zahteva sodelovanje:
  - tesnih poslovnih partnerjev
  - dobaviteljev
  - tretjih oseb
  - strank
  - drugih zunanjih partnerjev

Vzpostavitev varnostnih zahtev

- trije glavni viri varnostnih zahtev so:
  - analiza tveganj z upoštevanjem poslovne strategije in ciljev
  - zunanje zahteve: predpisi, pogodbe, družbeno okolje
  - lastni nabor principov, ciljev in poslovnih zahtev, ki jih je razvila organizacija sama

Analiza tveganj

- varnostne zahteve identificiramo z metodično analizo varnostnih tveganj
- stroški kontrol morajo biti usklajeni s potencialno škodo
- analizo tveganj izvajamo periodično zaradi sprememb v okolju in organizaciji

Izbira kontrol

- po vzpostavitvi varnostnih zahtev, opravljeni analizi tveganj, sprejetju odločitev za zmanjšanje tveganj
  - izberemo jih iz standarda,
  - drugih naborov kontrol,
  - lahko razvijemo svoje

Začetna točka vpeljave informacijske varnosti

- začetno točko vpeljave običajno izberemo glede na predpise ali pa običajno prakso informacijske varnosti.
- s stališča predpisov je to običajno:
  - zaščita podatkov in varstvo osebnih podatkov
  - zaščita organizacijskih zapisov
  - zaščita intelektualne lastnine

Običajna praksa informacijske varnosti

- politika informacijske varnosti
- določitev odgovornosti na področju informacijske varnosti
- zavedanje na področju informacijske varnosti, izobraževanje
- pravilna obdelava v aplikacijah
- tehnično upravljanje tveganj
- upravljanje neprekinjenega poslovanja
- upravljanje incidentov in izboljšav

Kritični dejavniki uspeha

- politika informacijske varnosti, cilji, aktivnosti, ki odražajo poslovne cilje
- pristop in ogrodje za implementacijo, vzdrževanje, spremljanje in izboljševanje informacijske varnosti, skladno z organizacijsko kulturo
- podpora in sodelovanje vseh ravni upravljanja
- dobro razumevanje tveganj, analize tveganj in upravljanja tveganj

Kritični dejavniki uspeha

- učinkovito osveščanje o informacijski varnosti vodstvenih delavcev, zaposlenih in drugih vpletenih za doseganje zavedanja
- distribucija smernic varnostne politike in standardov vsem vodstvenim delavcem, zaposlenim in drugim vpletenim
- zavezanost financiranja aktivnosti varovanja informacij

Kritični dejavniki uspeha

- zagotavljanje primerne stopnje zavedanja, izobraževanje
- vzpostavitev učinkovitega procesa upravljanja z incidenti
- vzpostavitev sistema merjenja za ocenjevanje učinkovitosti upravljanja varovanja informacij

Ocena tveganja

Vrste groženj

- Grožnje podatkom
  - razkritje
  - Izguba celovitosti (integritete)
  - Zavrnitev storitve (Denial of Service)
- Grožnje organizacijam
  - Izguba zaupanja
  - Osramočenje
  - Napaka pri upravljanju
- Grožnje infrastrukturi
  - Izpad napajanja

Ocena tveganj

- ocena tveganj
  - identificira,
  - kvantificira in
  - prioretizira tveganja
- glede na kriterije sprejemljivosti tveganj in
- cilje organizacije

Rezultati ocene tveganj

- rezultati vodijo in določajo:
  - primerne ukrepe in
  - prioritete
- uvajanja kontrol za zmanjševanje tveganj
- proces ocene tveganj je včasih treba ponoviti večkrat za različne dele organizacije ali posamezne informacijske sisteme
- oceno tveganj periodično ponavljamo

Vnaprej definiran obseg

- obseg mora biti natančno definiran
  - zaradi učinkovitosti in uspešnosti
  - povezati z oceno tveganj na drugih področjih, če obstaja
- obseg je lahko:
  - cela organizacija
  - deli organizacije
  - posamezni informacijski sistem
  - posamezne sistemske komponente
  - storitev

Naslavljanje tveganj

- najprej določimo kriterije za sprejemanje tveganj
- možni ukrepi za zmanjševanje tveganj so:
  - vzpostavitev kontrol za zmanjšanje tveganj
  - sprejemanje tveganj - odločitev o sprejemanju tveganja mora biti zabeležena in temeljiti na objektivnem merilu
  - izogibanje tveganj - ne uporabljamo aktivnosti, zaradi katerih se tveganje pojavi
  - prenos tveganja - npr. zavarovanje

Vzpostavitev kontrol

- mora ustrezati zahtevam iz ocene tveganj
- morajo zmanjšati tveganja na sprejemljivo raven ob upoštevanju:
  - zahtev in omejitev lokalnih in mednarodnih predpisov
  - organizacijskih ciljev
  - operativnih zahtev in omejitev
  - stroškov vzpostavitve in izvajanja kontrole - ohranitev razmerja z organizacijskimi zahtevami in omejitvami
  - uskladitev stroškov s potencialno škodo

Kdaj načrtujemo kontrole?

- v času specifikacije projektov in sistemov
- če tega ne upoštevamo:
  - povečani stroški
  - manj učinkovite rešitve
  - tudi možnost, da ne dosežemo ciljne ravni varnosti

Definicije

- Ranljivost: Karakteristika (pomanjkljivost) informacijske množice, ki jo lahko izkoristimo in zato predstavlja tveganje
  - Ranljivost sistema, ki jo je mogoče izkoristiti.
- Tveganje: Morebitna posledica nepričakovanega dogodka, ki lahko prizadene določen sistem.
  - Način, kako izkoristiti ranljivost.

Analiza tveganja

Analiza tveganja je proces, ki preverja sistem in njegove komponente z namenom odkrivanja ranljivosti in njihovih morebitnih posledic.

- Študija tveganj za določen poslovni ali informacijski sistem.
- Proces ugotavljanja izpostavljenosti in morebitne izgube.

Posledice tveganja

- Uničenje (podatkov, opreme, zgradb, ipd.);
- Popačenost ali sprememba (podatkov, aplikacij);
- Kraja, odtujitev ali izguba (opreme, podatkov, aplikacij);
- Nehoteno razkritje (podatkov);
- Neprimerna uporaba (nedovoljena programska oprema);
- Prekinitev delovanje ali storitev.

Primer: Odpoved trdega diska

Ocenitev, da bo trdi disk odpovedal v povprečju v treh letih.

- Verjetnost je 1/3 na leto
  - Stroški trdega diska so ok. 150€ (cena novega TD).
  - Upoštevamo tudi recimo 10 ur izgube – nalaganje OS, programske opreme in vzpostavitev sistema z varnostne kopije.
  - Dodatno že 4 ure zaradi prilagoditev, ki so bile potrebne, kjer smo vzpostavili sistem z varnostne kopije.
  - Predpostavimo, da je cena ure 20€.
- Celotna izguba = 150€ + 20€ x (10h + 4h) = 430€

Pričakovana letna izguba (PLI): (430€ x 1/3) = 143€/leto

Primer: Incident z trojanskim konjem

- Pogosto menjujete datoteke z znanci, a nimate nameščene protivirusne zaščite.
  - Predpostavimo, da se napad s trojanskim konjem dogodi vsakih 6 mesecev – verjetnost na leto je torej 2
  - Ni potrebe, da kupimo nov trdi disk.
  - Vzpostavitev sistema po napadu (10 + 4) ur,
- Celotna izguba = 20€ x (10+4) = 280€
- **PLI** = (280€ x 2) = 560€/leto

Varnostne politike

Kaj je varnostna politika?

Varnostna politika je skupek dokumentov, ki opisujejo postopke in vloge v procesu varovanja informacij

- vodilo vodstvene strukture podjetja, ki definira, kaj, kako in kdo je odgovoren za varno upravljanje informacij
- Obravnava več standardov:
  - ISO/IEC 27001:2005

Kaj je varnostna politika?

- Varnostna politika določa pravila vsem zaposlenim: uporabnikom informacijskega sistema, upravi in skrbnikom sistema. Z varnostno politiko:
  - preverjamo trenutno stanje varnosti informacijskih sistemov,
  - definiramo postopke za komunikacijo z zunanjimi partnerji,
  - dokazujemo ustreznost zaščite informacij in skladnost z zakonodajo,
  - imamo pogoj za pridobitev certifikata po standardu ISO/IEC 27001:2005

Načrtovanje VP

- V osnovi moramo pri varovanju informacij upoštevati:
  - razumevanje groženj,
  - opisati ustrezne vrste zaščite informacij, s katerimi preprečimo izgube, kraje uničenje, korupcijo itd.,
  - biti pripravljeni, da v primeru nesreč le te zmanjšamo na čim manjšo škodo,
  - znati oceniti škodo, identificirati izvor kršitve in jo znati tudi popraviti,
  - znati se hitro opomoči od napada, pregledati in popraviti varnost informacij.

Cilji VP

- varovati informacijska sredstva podjetja pred krajo, zlorabo ali kakršno koli obliko poškodbe,
- jasno opredeliti področja odgovornosti in obveznosti uporabnikov, skrbnikov in vodilnih,
- dovoliti pooblaščen dostop in preprečevati nepooblaščeni dostop do informacij,
- biti implementirana skozi sistemske skrbniške postopke, smiselne smernice, ali druge primerne metode,
- omogočati uvajanje varnostnih mehanizmov in orodij oziroma implementirati sankcije, kjer preventivni postopki tehnično niso izvedljivi,

Cilji VP

- jasno opredeliti področja odgovornosti uporabnikov, skrbnikov in vodilnih,
- biti predstavljena vsem v okviru organizacije,
- biti prilagodljiva spremembam okolja informacijske tehnologije, saj je živ dokument, ki se nenehno nadgrajuje,
- spodbujati vodstvo in zaposlene, da ohranjajo potrebno raven znanja za varovanje informacij,
- omogočati, da podjetje nadaljuje z delom, kljub pomembni kršitvi informacij.

Obseg VP

- Varnostna politika naj bi tako pokrivala naslednja področja:
  - varnost strojne opreme (hardware), perifernih naprav in ostale opreme,
  - nadzor dostopa do informacij in sistemov (pooblaščen in nepooblaščen dostop),
  - procesiranje dokumentov in informacij,
  - kupovanje in vzdrževanje programske opreme (software),
  - razvijanje in vzdrževanje domačih programov,

Obseg VP

- implementacijo skozi sistemske skrbniške postopke, smiselne smernice, ali druge primerne metode,
- uvajanje varnostnih mehanizmov in orodij,
- izobraževanje zaposlenih in njihova seznanitev z varovanjem informacij,
- odkrivanje in odzivanje na pripetljaje glede varnosti,
- opredelitev ravnanja v primeru kršenja politike,
- ipd.

Vrste varnostne politike

- Varnostna politika se vpleta v več plasti, vendar jo lahko razdelimo na tri glavna področja.
  - ***Upraviteljski del*** - Obsega pripravo in sprotno usklajevanje in dopolnjevanje dokumentacije s področja varnostne politike za informacijsko tehnologijo.
  - ***Izvedbeni del*** - Obsega dejansko implementacijo standardov, smernic in postopkov v operativnem okolju informacijskega sistema.
  - ***Nadzorni del*** - Obsega nadzor in spremljanje izvajanja sprejete varnostne politike za informacijsko tehnologijo.

Področja VP

- *Fizična zaščita* – naravne nesreče, vsiljivci, kontrola vstopov, varovanje pisarn (zaklepanje. Ognjevarne omare). Zaščita pred požarom, vodo in naravnimi nesrečami, UPS, …
- *Računalnik (strežnik, odjemalec, delovna postaja, ipd.)* – posodabljanje OS in ostale programske opreme, spisek naprav in nameščenih programov, politika nameščanja SW, varnostne kopije, …
- *Virusi in škodljivi programi* – opredelimo namestitev ustreznih varnostnih programov (protivirusni, požarni zidovi, ipd.)

Področja VP

- *Internet* - omejitev interneta na minimum, potreben za delo
- *Gesla* - dolžina in kakovost gesel, pogostost menjavanja gesel
- *Elektronska pošta* - kaj je dovoljeno pošiljate in kaj ne, kako varovati el. pošto (gesla)
- *Prenos podatkov* - katere medije lahko uporabljamo (npr. USB ključke), pravice uporabe tiskalnikov
- *Pomoč uporabnikom* - izobraževanja, ustanoviti center za pomoč uporabnikom (help desk)